Uninett CERT RFC 2350 profile

1 Document Information

This document is compliant with RFC 2350.

1.1 Date of Last Update

This is version 1.1, 2018-05-15

1.2 Distribution List for Notifications

This profile is kept up-to-date on the location specified in section 1.3.
E-mail notifications of updates are sent to the Trusted Introducer for CERTs in Europe (see https://www.trusted-introducer.org/).

1.3 Locations where this Document may be found

The current version of this profile is available at https://www.uninett.no/cert/rfc2350.

2 Contact Information

2.1 Name of the Team

Uninett CERT

2.2 Address

Postal address:

Uninett CERT
PO box 4769 Torgard
NO-7465 Trondheim
Norway

2.3 Time Zone

Nominally CET (UTC +1), CEST (UTC +2) during daylight saving time.

2.4 Telephone Number

+47 73 55 79 60

2.5 Facsimile Number

+47 73 55 79 01

2.6 Other Telecommunication

Not applicable

2.7 Electronic Mail Address

Main e-mail address for incident-related communication: cert@uninett.no.
For communication not related to incidents, please use cert-info@uninett.no.

2.8 Public Keys and Encryption Information

Please encrypt any sensitive information with the Uninett CERT team key.
The current key can be found at https://www.uninett.no/cert/uninett-cert.asc

Please sign your messages using your own key, which should be verifiable through public key servers.

2.9 Team Members

This information is available only to TI accredited teams, see
https://tiw.trusted-introducer.org/teams/data/uninett-cert.html

2.10 Other Information

Uninett CERT is accredited by the Trusted Introducer for CERTs in Europe, see https://www.trusted-introducer.org/teams/uninett-cert.html for details.

Uninett CERT is a member of the Forum of Incident Response and Security Teams (FIRST), see https://www.first.org/members/teams/uninett_cert for details.

3 Points of Customer Contact

E-mail is the preferred method for contacting Uninett CERT.

- For incident related communication, including incident reports, please use cert@uninett.no.
- For general inquiries, please use cert-info@uninett.no.
- Telephone during business hours (08:00–16:00 CET/CEST Monday–Friday): +47 73 55 79 60.
- Telephone for time-critical emergencies outside business hours: +47 911 27 087.

4 Charter

4.1 Mission Statement

The purpose of Uninett CERT is to prevent and minimize damage from IT security related incidents in the Norwegian higher education sector.
Uninett CERT shall assist technical staff that are responsible for maintenance or development of networks, infrastructure, and information systems – at Uninett and Uninett's customers – in the prevention, detection, and handling of security incidents.
Uninett CERT is given the authority to independently implement necessary precautions to protect network, infrastructure, and IT resources in conjunction with IT security incidents, cf. Uninett's policy for acceptable use (AUP).

4.2 Constituency

Uninett is the Norwegian NREN (national research and education network), and the services of Uninett CERT are available to all of Uninett's customers.

4.3 Sponsorship and/or Affiliation

Uninett CERT is part of and fully financed by Uninett.

4.4 Authority

If the Uninett AUP is violated, e.g. if activities on a customer's internal network constitutes a problem for Uninett or other parties, Uninett CERT has the authority to take relevant countermeasures. In particular, Uninett CERT may block certain hosts or the institution's entire network from accessing the Internet.

5 Policies

5.1 Types of Incidents and Level of Support

All incidents are initially considered normal priority. Uninett CERT will assess incidents based on severity and impact on the constituency.

5.2 Co-operation, Interaction and Disclosure of Information

Classification
Sensitive information encompasses sensitive personal data, as defined by relevant privacy legislation, and business confidential information. All information related to security incidents is considered sensitive, unless all concerned parties specifically state otherwise.
Non-sensitive information consists of publicly available (open) information.

Information handling
Sensitive information is stored and communicated securely. Sensitive information brought to the team's knowledge may be distributed amongst the Uninett CERT team members. Members of Uninett CERT are subject to explicit non-disclosure agreements regarding all sensitive information.

Information disclosure
In order to investigate and resolve security incidents, incident related information may be released to appropriate parties on a strictly need-to-know basis, and preferably anonymized. Non-sensitive information may be distributed to the general public on a need-to-know basis.

Legal considerations
Uninett is not subject to the Norwegian Telecommunications Act which states that logs should be handed over to the authorities on request, without any prior court order. However, Uninett CERT will in general cooperate with law enforcement authorities during investigation of possible criminal activity relevant to our constituency, and providing e.g. event and system logs. Sensitive information can be

handed over to relevant authorities following a court order.

Traffic Light Protocol (ISTLP)

Uninett CERT supports the Traffic Light Protocol (ISTLP), and all tagged information will be handled in accordance with https://www.first.org/tlp.

5.3 Communication and Authentication

See 2.8 above.

Uninett CERT uses PGP/GPG to ensure the confidentiality and integrity of sensitive information. Normally, all information provided by Uninett CERT is digitally signed with the team key, and sensitive information is encrypted. It is highly recommended to use PGP/GPG in all cases where sensitive information is involved. Norwegian authorities does not enforce restrictions on key sizes or the use of cryptography, and there are no key escrow requirements.

6 Services

6.1 Incident Response

Uninett CERT can assist system administrators in handling the technical and organizational aspects of computer security incidents.

6.1.1 Incident Triage

- Investigating whether indeed an incident occurred.
- Determining the extent of the incident.

6.1.2 Incident Coordination

- Contacting the involved customer institution(s).
- Determining the initial cause of the incident.
- Contacting other members of the constituency that may be involved in or exposed to the particular threat.
- Composing announcements to users, if applicable.
- Making reports to other CSIRTs, if applicable

6.1.3 Incident Resolution

- For incidents occurring at customer institutions, Uninett CERT typically assumes an advisory role.
- For internal incidents, the following relevant steps are taken:
  - Remove the vulnerability.
  - Secure the system from the effects of the incident.
  - Collect evidence after the fact, if applicable.
  - Take appropriate countermeasures to protect against recurring incidents.

- Wrap-up, lessons learned.

6.2 Proactive Activities

- Uninett maintains the security mailing list sikkerhet-info@uninett.no which customer organizations can subscribe to. Information that is considered relevant for a significant part of the constituency is published on this list.
- Configuration and maintenance of security-related tools, applications, and infrastructure.
- Non-intrusive monitoring of network traffic for indications of misuse.
- Uninett CERT has a regular column in the constituency newsletter Uninytt.
- Regular presentations during the annual Uninett conference.

Please send incident reports to cert@uninett.no. Encrypting sensitive information is highly encouraged.

7 Disclaimers

None.